

Basic Axioms and Examples

Note 1

cca4f1927b2c4eeaa3123dbcf0680bc0

Given a set G , $\{\{c2:: \text{a binary operation } \star \text{ on } G\}\}$ is $\{\{c1:: \text{a function}$

$$\star : G \times G \rightarrow G.$$

$\}\}$

Note 2

7732d25ebb1e40dd9696c1c921803c17

Given a binary operation \star on a set G , for any $a, b \in G$ we shall write $\{\{c2:: a \star b\}\}$ for $\{\{c1:: \star(a, b),.\}\}$

Note 3

4fc60827250f4af4ab6a669ac7632568

A binary operation \star on a set G is $\{\{c2:: \text{associative}\}\}$ if $\{\{c1:: \text{for all } a, b, c \in G \text{ we have}$

$$a \star (b \star c) = (a \star b) \star c.$$

$\}\}$

Note 4

192d8d86f22349cabcd9f1a229fc45290

If \star is a binary operation on a set G we say elements a and b of G $\{\{c1:: \text{commute}\}\}$ if $\{\{c2::$

$$a \star b = b \star a.$$

$\}\}$

Note 5

e5cbf512d6a54c91950c65450a07a501

A binary operation \star on a set G is $\{\{c2:: \text{commutative}\}\}$ if $\{\{c1:: \text{for all } a, b \in G \text{ we have}$

$$a \star b = b \star a.$$

$\}\}$

Note 6

36b096eebd7f4264ab071a5fa4cfe13

Suppose that \star is a binary operation on a set G and $H \subseteq G$. If $\{\{c2:: \text{the restriction of } \star \text{ to } H \text{ is a binary operation on } H,\}\}$ then H is said to be $\{\{c1:: \text{closed under } \star,\}\}$

Note 7

644b1cd8fa014885ad295ae5c089e5a7

A group is an ordered pair (G, \star) where G is a set and \star is a binary operation on G satisfying the group axioms.

Note 8

5de4e717b4814adf8acd4f8d9a93322c

How many axiom are there in the definition of a group (G, \star) ?

■ Three.

Note 9

2dc690f5008a4b8c8691c36308e44295

What is the first axiom from the definition of a group (G, \star) ?

■ \star is associative.

Note 10

4fcc137e66a048459cc73d6735e4ccea

Given a binary operation \star on a set G , an element $e \in G$ is called an identity of G if for all $a \in G$ we have

$$a \star e = e \star a = a.$$

}

Note 11

a3cd125f152f432082757242096a76ef

What is the second axiom from the definition of a group (G, \star) ?

■ There exists an identity of G .

Note 12

5d438f0c3fb24b1a97507e81f868846e

Given a binary operation \star on a set G and $a \in G$, an element $\tilde{a} \in G$ is called an inverse of a if

$$a \star \tilde{a} = \tilde{a} \star a = e.$$

}

Note 13

d840b7b910d740f3bea231c74feba51c

Given a binary operation \star on a set G and $a \in G$, $\{c2::\text{an inverse of } a\}$ is usually denoted $\{c1::a^{-1},\}$

Note 14

c4c56a11c6f746b3ae287ec386b4e12b

What is the third axiom from the definition of a group (G, \star) ?

■ For all $a \in G$ there exists a^{-1} .

Note 15

be05e23d350d4f49a65602b65045f888

A group (G, \star) is called $\{c2::\text{abelian}\}$ if $\{c1::\star \text{ is commutative.}\}$

Note 16

978f23382d594a28a3de168b7f661c30

We shall say G is $\{c2::\text{a group under } \star\}$ if $\{c1::(G, \star) \text{ is a group.}\}$

Note 17

497f01593d7f4ffabb546b455788b354

We shall say a set G is $\{c2::\text{a group}\}$ if $\{c1::G \text{ is a group under an operation that is clear from the context.}\}$

Note 18

61ea2504ca474fe4aae902eb1965576c

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and \mathbb{C} are $\{c2::\text{groups}\}$ under $\{c1::+\}$

Note 19

84b6a231d3934ab3b4f63226549a9589

$\mathbb{Q} - \{0\}, \mathbb{R} - \{0\}, \mathbb{C} - \{0\}$ are $\{c2::\text{groups}\}$ under $\{c1::\times.\}$

Note 20

3051cd354f5040e2bdf0809e005635ed

$\mathbb{Q}^+, \mathbb{R}^+$ are $\{c2::\text{groups}\}$ under $\{c1::\times.\}$

Note 21

21f924e833cd4e0bbae5f4588dff47b5

Is $\mathbb{Z} - \{0\}$ a group under \times ?

■ No. (There is no inverse.)

Note 22

edec2a960f6d43dbb5e19283c28db7bd

Let V be a vector space. Then V is $\{\{c2: \text{a group}\} \text{ under } \{\{c1: +, \cdot\}\}$

Note 23

47a03e2c688244b1b3a5126fd04a21c7

Let $n \in \mathbb{Z}^+$. Then $\{\{c3: \mathbb{Z}/n\mathbb{Z}\} \text{ is } \{\{c2: \text{a group}\} \text{ under } \{\{c1: \text{addition}\}\} \text{ of residue classes.}$

Note 24

f6a5a40cfee6495dae0d36f7b3288cb2

Let $n \in \mathbb{Z}^+$. Then $\{\{c3: (\mathbb{Z}/n\mathbb{Z})^\times\} \text{ is } \{\{c2: \text{a group}\} \text{ under } \{\{c1: \text{multiplication}\}\} \text{ of residue classes.}$

Note 25

3e94ca73ca344269bb98d94a22204fd9

If (A, \star) and (B, \diamond) are $\{\{c4: \text{groups},\}\}$ then the group $\{\{c2: A \times B,\}\}$ whose operation is $\{\{c1: \text{defined componentwise:}$

$$(a, b)(c, d) = (a \star c, b \diamond d),$$

$\}\}$ is called $\{\{c3: \text{the direct product of the two groups.}\}\}$

Note 26

e23d8e577b3948af9b0cadd5df7c9141

If (G, \star) is a group, then $\{\{c2: \text{the identity of } G\} \text{ is } \{\{c1: \text{unique.}\}\}$

Note 27

5b5391986e9b49ea9c5f9f73813e9594

If (G, \star) is a group, then the identity of G is unique. What is the key idea in the proof?

■ Consider the product of two arbitrary identities.

Note 28

0989a259fae446c48bb0f6c40394efd0

If (G, \star) is a group, then for every $a \in G$, $\{\{c2: a^{-1}\}\}$ is $\{\{c1: \text{uniquely determined.}\}\}$

Note 29

f0b0a651592c466ba8067beb3b1570b8

If (G, \star) is a group, then for every $a \in G$, a^{-1} is uniquely determined. What is the key idea in the proof?

■ Multiply an inverse on the right by $a \star a^{-1}$.

Note 30

4a6a6806d8874839bb7956d76e384333

If (G, \star) is a group and $a \in G$, then

$$(a^{-1})^{-1} = \{\{c1::a.\}\}$$

Note 31

9ab0e972d6a24baea99f1577cbf03423

If (G, \star) is a group and $a, b \in G$, then

$$\{\{c2::(a \star b)^{-1}\}\} = \{\{c1::(b^{-1}) \star (a^{-1}).\}\}$$

Note 32

69b3db6e70ad4629aa55a855b8df8096

If (G, \star) is a group and $a_1, \dots, a_n \in G$, then the value of

$$a_1 \star \dots \star a_n$$

is $\{\{c2::\text{independent}\}\}$ of $\{\{c1::\text{how the expression is bracketed.}\}\}$

« $\{\{c3::\text{The generalized associative law}\}\}$ »

Note 33

05cc8fd523084650adb46704dde222a7

What is the key idea in the proof of the generalized associative law for a group (G, \star) ?

■ By induction.

Note 34

9ca193d1531c4c49b296732d7ff12fb5

Henceforth our abstract groups G, H , etc. will always be written with the operation as $\{\{c1::\cdot.\}\}$

Note 35

7d06acac21c14a628ad1ccb470fe6398

Henceforth for an abstract group G (operation \cdot) an expression $\{\{c2::a \cdot b\}\}$ will always be written as $\{\{c1::ab\}\}$

Note 36

0994e6080f3042ad81bc90d1ced0b747

Henceforth for an abstract group G (operation \cdot) we denote $\{\{c2::$ the identity of $G\}\}$ by $\{\{c1::1\}\}$

Note 37

361c99f13a9b4304868fdb350b45dbf

For any group G and $x \in G$ and $\{\{c3::n \in \mathbb{Z}^+\}\}$ we shall denote by $\{\{c2::x^n\}\}$ $\{\{c1::$ the product

$$\underbrace{xx \cdots x}_{n \text{ terms}}$$

$\}\}$

Note 38

5b7f3c41cf0147e2bffc3929ed9ec480

For any group G and $x \in G$ and $\{\{c3::n \in \mathbb{Z}^+\}\}$ we shall denote by $\{\{c2::x^{-n}\}\}$ $\{\{c1::$ the product

$$\underbrace{x^{-1}x^{-1} \cdots x^{-1}}_{n \text{ terms}}.$$

$\}\}$

Note 39

a7a44229ce0f4a4b11d1410dc0fab0f

For any group G and $\{\{c3::x \in G\}\}$ let $x^{\{\{c2::0\}\}} \stackrel{\text{def}}{=} \{\{c1::1, \text{ the identity of } G\}\}$.

Note 40

b1be1b97f53c45fa9451caa7112ca406

Let G be a group and let $a, u, v \in G$. Then $au = av$ $\{\{c2::$ if and only if $\}\}$ $\{\{c1::u = v\}\}$

« $\{\{c3::$ Cancellation rule $\}\}$ »

Note 41

ed8673154d544c7b86ac358facc79101

For G a group and $x \in G$ define the order of x to be the smallest positive integer n such that

$$x^n = 1.$$

}}

Note 42

8c334a6360be4bec8fae7f712ab2c4ee

For G a group and $x \in G$, if no positive power of x is the identity, the order of x is defined to be infinity.

Note 43

ba4143a322564f8383f6e7d91ca32a75

For G a group and $x \in G$, denote the order of x by $|x|$.

Note 44

d7fee5bcbdbd47bcb6f4a2ba086fa2ed

For G a group and $x \in G$, if the order of x is an integer n , x is said to be of order n .

Note 45

db12c606699d40e89d499d554bd52b28

For G a group and $x \in G$, if the order of x is infinite, x is said to be of infinite order.

Note 46

2e514c62ce4e48eb9c6bd3b5de1d7c44

An element of a group has order 1 if and only if it is the identity.

Note 47

babeb7cf1b394be6a4f8d86e1a099cda

Let $G = \{g_1, g_2, \dots, g_n\}$ be a finite group with $g_1 = 1$. The multiplication table or group table of G is the matrix

$$\begin{bmatrix} g_i g_j \end{bmatrix} \sim n \times n.$$

}}

Note 48

f245736b42b44f178f9a1d661bc4a5c7

Let $G = \{x \in \mathbb{R} \mid x \in [0, 1)\}$ and for $x, y \in G$ let $x \star y$ be the fractional part of $x + y$. Then the group (G, \star) is called the real numbers mod 1.

Note 49

3664191737c844f38816547b7acd64c1

Let $G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$. Then the group $(G, +)$ is called the group of roots of unity in \mathbb{C} .

Note 50

85c981d4f1564164bb547096829d245b

A finite group is abelian if and only if its group table is a symmetric matrix.

Note 51

859ef5188ad14b35b58dc9428333e5ad

Let G a group and $x \in G$ and $a, b \in \mathbb{Z}$. Then $x^{a+b} = x^a x^b$.

Note 52

0c6c419e61fc48139ff6afd4a8e28be6

Let G a group and $x \in G$. Then $|x^{-1}| = |x|$.

Note 53

f221410dc76e4c7881175d62226ecd4

Let G a group and $x, g \in G$. Then $|g^{-1}xg| = |x|$.

Note 54

9951f3d62ec841df9c6f8cfc07f3c04f

Let G a group and $a, b \in G$. Then $|ba| = |ab|$.

Note 55

b30a94de99fe4c2f91b5417fdbb3e99d

Let G a group, $x \in G$, $|x| = n < \infty$ and $s \in \mathbb{Z}$. Then $x^s = 1$ if and only if $n \mid s$.

Note 56

5a0539b7021242e2a9a5769a1c156889

Let G a group, $x \in G$, $|x| = n < \infty$ and $s \in \mathbb{Z}$. Then

$$|x^s| = \frac{n}{(n, s)}.$$

Note 57

7ec585d338e941d7b465cf11d0f42550

Let G a group, $x \in G$, $|x| = n < \infty$ and $s \in \mathbb{Z}$. Then $|x^s| = \frac{n}{(n,s)}$.
What is the key idea in the proof?

■ $(x^s)^k = 1$ if and only if $n \mid sk$.

Note 58

00c58492691e442b9a8c0a5ba21a0c7f

Let G a group, $x \in G$. If $x^2 = 1$ then

$$x^{-1} = \langle\langle c1: x. \rangle\rangle$$

Note 59

89199067c84244c094af347afff31c8a

Let G a group. If $\langle\langle c3: a \text{ and } b \text{ are commuting elements of } G \rangle\rangle$ then
 $\langle\langle c2: (ab)^n \rangle\rangle = \langle\langle c1: a^n b^n \rangle\rangle$.

Note 60

87374145922242e3a5bc43fa952448dc

Let G a group. If $x^2 = 1$ for all $x \in G$ then G is $\langle\langle c1: \text{abelian.} \rangle\rangle$

Note 61

cdf7b8b7731c4e619920d66f7520b423

Let G a group. If $x^2 = 1$ for all $x \in G$ then G is abelian. What is the key idea in the proof?

■ $1 = (ab)^2$ and multiply by a on the left and by b on the right.

Note 62

c48695948e6a4cf69846a629c6b45cb5

Let (G, \star) be a group and $\langle\langle c4: H \subseteq G. \rangle\rangle$ If $\langle\langle c2: H \text{ is a group under the operation } \star \text{ restricted to } H \rangle\rangle$ then $\langle\langle c3: H \rangle\rangle$ is called $\langle\langle c1: \text{a subgroup of } G. \rangle\rangle$

Note 63

39703ef9887d48e9b763bea0c6519b19

Let G a group and $\langle\langle c3: x \in G. \rangle\rangle$ Then $\langle\langle c2: \text{the subgroup } \{x^n \mid n \in \mathbb{Z}\} \text{ of } G \rangle\rangle$ is called $\langle\langle c1: \text{the cyclic subgroup of } G \text{ generated by } x. \rangle\rangle$

Note 64

7d1e317bc7c64c538d09a6fd6c2e2011

Let A and B be groups. Then $A \times B$ is abelian if and only if both A and B are abelian.

Note 65

c048d6c9ce83411c94e040e5991b3524

Let A and B be groups, $(a, b) \in A \times B$. Then the order of (a, b) is the least common multiple of $|a|$ and $|b|$.

Note 66

de71dcf7adc64bcd9b53502c90a0cefa

Let A and B be groups, $(a, b) \in A \times B$. Then

$$(a, b)^k = (a^k, b^k)$$

for all $k \in \mathbb{Z}$.

Note 67

e672cc6907124507a4fd998675844d02

Let A and B be groups, $(a, b) \in A \times B$. Then the order of (a, b) is the least common multiple of $|a|$ and $|b|$. What is the key idea in the proof?

■ $(a, b)^k = (a^k, b^k).$

Note 68

e6f9e981e45d4f55a3aafa3eb6d77ef1

Any finite group of even order contains an element of order 2.

Note 69

d13862b410194166829309d8ea4880a6

Any finite group of even order contains an element of order 2. What is the key idea in the proof?

■ Show that the set $\{g \in G \mid g \neq g^{-1}\}$ has an even number of elements.

Note 70

86e37f9ff199460995332631a61f9a00

Let G a group, $x \in G$ and $|x| = n < \infty$. Then the elements $\{x^i : 0 \leq i < n\}$

$$1, x, x^2, \dots, x^{n-1}$$

are distinct.

Note 71

1bf4e9f2f854544bf96f1364e0064ed

Let G a group, $x \in G$ and $|x| < \infty$. Then $|x| \leq |G|$.

Note 72

5f4f77e21f2b4052979906547275dfd9

Let G a group, $x \in G$ and $|x| < \infty$. Then $|x| \leq |G|$. What is the key idea in the proof?

The elements $1, x, \dots, x^{n-1}$ are the only powers of x .

Note 73

4f07acc87f6949e092c057cb5a580c77

Let G a group, $x \in G$ and $|x| = \infty$. Then the elements $\{x^n : n \in \mathbb{Z}\}$

$$x^n, n \in \mathbb{Z}$$

are distinct.

Dihedral Groups

Note 1

c895ff9d20ae4a2286bb783680b3cee8

A symmetry of a regular n -gon is any rigid motion of the n -gon which can be effected by taking a copy of the n -gon, moving this copy in any fashion in 3-space and then placing the copy back on the original n -gon so it exactly covers it.

Note 2

3a08bb223d9241bbb5cd4dae15a4a23d

Each symmetry of a regular n -gon can be described uniquely by the corresponding permutation of $\{1, 2, \dots, n\}$, representing the permutation of the vertices.

Note 3

c0d6e6d3d60b45058b7957002e045102

Given $n \in \mathbb{Z}^+$ and $n \geq 3$, the group of symmetries of a regular n -gon is called the dihedral group of order $2n$.

Note 4

7a77331a22e144ceaf6ca7c1b475a99a

Given $n \in \mathbb{Z}^+$ and $n \geq 3$, the dihedral group of order $2n$ is denoted D_{2n} .

Note 5

a81873dbe4e6432f93bb1d8c3c5978f1

Given $n \in \mathbb{Z}^+$, $n \geq 3$ and $s, t \in D_{2n}$, the product st is defined to be the symmetry obtained by first applying t then s to the n -gon.

Note 6

1457d2279c1d432a9d371d8797d9b621

Given $n \in \mathbb{Z}^+$ and $n \geq 3$,

$$|D_{2n}| = 2n.$$

Note 7

af77787eb9d94bae94d7df59b0415212

Given $n \in \mathbb{Z}^+$ and $n \geq 3$, $|D_{2n}| = 2n$. What is the key idea in the proof?

Every symmetry is uniquely determined by how it affects some two adjacent vertices.

Note 8

1a3443407b8641c5adc691e47eef2f1e

For convenience, the regular n -gon viewed in D_{2n} is fixed centered at the origin.

Note 9

b85d695a3fff47fba9b07b7a341cd0

For convenience, the vertices of the regular n -gon viewed in D_{2n} are labeled consecutively from 1 to n in a clockwise manner.

Note 10

8005824717e34f4a8e154dfa84d25f17

In the context of the D_{2n} group, let r be the rotation clockwise about the origin through $2\pi/n$ radian.

Note 11

8439aae412044be9bf8f6c59334cd570

In the context of the D_{2n} group, let s be the reflection about the line of symmetry through vertex 1 and the origin.

Note 12

d46303ae65e74f2e8f610b873f4e559b

In the context of the D_{2n} group, is it possible that $s = r^i$ for some i ?

No.

Note 13

5aaf131bef484c89b455ce9f5b4a2eae

In the context of the D_{2n} group, is it possible that $sr^i = sr^j$ for some $i \not\equiv j \pmod{n}$?

■ No.

Note 14

79c14b3dba52416f934c9d820acb0be7

Each element of D_{2n} can be written uniquely in the form $s^k r^i$ for some $k = 0$ or 1 and $0 \leq i \leq n - 1$.

Note 15

f3a7147f62d84c53b1ecc4f7da081eba

In the context of the D_{2n} group,

$$r^i s = sr^{-i}, \text{ for all } 0 \leq i \leq n.$$

Note 16

2600f25fd1ec408b8e47e341dc6cdb64

In the context of the D_{2n} group,

$$r^i s = sr^{-i}, \text{ for all } 0 \leq i \leq n.$$

What is the key idea in the proof?

■ $rs = sr^{-1}$ and by induction.

Note 17

f56559b6eae841cea409f8438221c1b2

A subset S of elements of a group G with the property that every element of G can be written as a (finite) product of elements of S and their inverses is called a set of generators of G .

Note 18

d72e348121f94214980378f08a5e45a3

If S is a set of generators of a group G , we shall write

$$G = \langle S \rangle.$$

}}

Note 19

7bc8f288fd5d45e0a89eb59abdc95810

If S is a set of generators of a group G , we shall say G is generated by S .

Note 20

cb072c7b416e4fbf8e3cf95f496f4083

In terms of generators, the group $D_{2n} = \langle r, s \rangle$.

Note 21

4fd6980a252a486980db01306accceef

In a finite group G a set S generates G if every element of G is a finite product of elements of S .

Note 22

90b6154b7aaa48398ddecb91083d71ac

In the D_{2n} group, the relations $r^n = 1$, $s^2 = 1$ and $rs = sr^{-1}$ have the additional property that any other relation between elements of the group may be derived from these three.

Note 23

4681975ee07c4032a3ced2de0ccfa631

In the D_{2n} group, the relations $r^n = 1$, $s^2 = 1$ and $rs = sr^{-1}$ have the additional property that any other relation between elements of the group may be derived from these three. What is the key idea in the proof?

We can determine exactly when two group elements are equal by using only these three relations.

Note 24

b0bcc70704c64cccb8d832a4540749b

Let G be a group. Any equations in G that the generators satisfy are called relations in G .

Note 25

b8f9a5669c634d39ac14a6115f6b142d

Let G be a group. If G is generated by a subset S and there is some collection of relations such that any relation among the elements of S can be deduced from these, we shall call these generators and relations a presentation of G .

Note 26

265ab5c6f292430c8ecc6ab97f25c8a8

Let G be a group. If $\langle S \rangle$ is a subset S and $\{R_1, \dots, R_m\}$ a collection of relations R_1, \dots, R_m form a presentation of G , we shall write

$$G = \langle S \mid R_1, \dots, R_m \rangle.$$

}

Note 27

b8acfa74c7df4502a3b76c59342afbac

One presentation for the dihedral group D_{2n} is

$$\langle D_{2n} \rangle = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle.$$

Note 28

06f27cb1fae140be909a72d4d52162a8

If $n = 2k$ is even and $n \geq 4$ then $\langle r^k \rangle$ is the only nonidentity element of D_{2n} which commutes with all elements of D_{2n} .

Symmetric Groups

Note 1

35103f7401374322997a41574a878c47

Given a set Ω , $\{\{c1::\text{the set of all bijections from } \Omega \text{ to itself}\}\}$ is denoted $\{\{c2::S_{\Omega}\}\}$

Note 2

e190a5ea3cc542a09f5d22434fd383e7

Let Ω be a $\{\{c4::\text{nonempty}\}\}$ set. Then the group $(\{\{c2::S_{\Omega}\}\}, \{\{c3::\circ\}\})$ is called $\{\{c1::\text{the symmetric group on the set } \Omega\}\}$

Note 3

41b5292492ba47c2b0c6733f4d86e86e

Let $n \in \mathbb{Z}^+$. $\{\{c2::\text{The symmetric group on the set } \{1, 2, \dots, n\}\}\}$ is called $\{\{c1::\text{the symmetric group of degree } n\}\}$

Note 4

b7fae74ed3df4e71b785bd65d2e5e42b

Let $n \in \mathbb{Z}^+$. $\{\{c2::\text{The symmetric group of degree } n\}\}$ is denoted $\{\{c1::S_n\}\}$

Note 5

40a80f61353b460c9200ea835050fc6d

Let $n \in \mathbb{Z}^+$. Then

$$|S_n| = \{\{c1::n!\}\}$$

Note 6

971a7ee9395248c3ad6b53fc7e57223c

$\{\{c3::\text{A cycle}\}\}$ is $\{\{c1::\text{a string of integers}\}\}$ which represents the element of S_n which $\{\{c2::\text{cyclically permutes these integers (and fixes all other integers)}\}\}$

Note 7

0d979e8f5d444cd2b20479e738e3b244

$\{\{c2::\text{The cycle } (a_1 \ a_2 \ \dots \ a_m)\}\}$ in S_n is $\{\{c1::\text{the permutation}$

$$a_i \mapsto a_{i+1} \quad a_m \mapsto a_1.$$

$\}\}$

Note 8

1ecd3b35c9e34999a9cd7481ad891e0d

The length of a cycle in S_n is the number of integers that appear in it.

Note 9

d53a85a6dc624da7b74414131a5c9b0b

A cycle of length t in S_n is called a t -cycle.

Note 10

69e31cdb5b8644e790c3368b3b37f9fc

Two cycles in S_n are called disjoint if they have no numbers in common.

Note 11

d1990b072a9244dca0f3ae3ea60a5bf0

Let $\sigma \in S_n$. The representation of σ as the products of pairwise disjoint cycles is called the cycle decomposition of σ .

Note 12

562293a2603f483ab79fd4e9cbd6d36e

The identity permutation of S_n will be written as 1 .

Note 13

2e6d113b0fdf478f9cacb6d733a989c3

S_n is a non-abelian group for all $n \geq 3$.

Note 14

3ff49b43f20f4b3390f3e555c41492a1

Disjoint cycles in S_n commute.

Note 15

6c2a6cc5ad27457db08edcca242f5353

The cycle decomposition of each permutation in S_n is the unique way of expressing a permutation as a product of disjoint cycles (up to rearrangement).

Note 16

f1f1d98922ba4affa25f8a1500989973

The order of a permutation in S_n is the l.c.m. of the lengths of the cycles in its cycle decomposition.

Note 17

e539f64a563146f68a90f700cee3c2a6

Let σ be a k -cycle in S_n . Then

$$|\sigma| = \{c1:k.\}$$

Note 18

0f104518132a45bf947b3861439a4677

Let σ be a k -cycle in S_n . For which positive integers i is σ^i also a k -cycle?

■ For i relatively prime to k .

Note 19

2c81a75df4394dd8945d760a2dd538a3

Let σ be a k -cycle in S_n . What is special about the cyclic decomposition of σ^i for an arbitrary $i \in \mathbb{Z}^+$?

■ All of the disjoint cycles have the same length and are “evenly spaced.”

Note 20

a6f4e4da4d104be3b33ee481ae4a34fc

Let p be $\{c3:a \text{ prime.}\}$ An element has order $\{c2:p\}$ in S_n if and only if $\{c4: \text{its cycle decomposition}\}$ is $\{c1: \text{a product of commuting } p\text{-cycles.}\}$

Matrix Groups

Note 1

d24745203ab949c39f465e4e32838554

First, a field is $\{\{c2::a \text{ set } F\}\}$ together with $\{\{c1::\text{two binary operations } + \text{ and } \cdot \text{ on } F.\}\}$

Note 2

f3c03aa477f94f80bb772b9ea31136f9

How are the properties of $+$ summarised in the definition of a field F ?

■ $(F, +)$ is an abelian group.

Note 3

dace43278a624b1a8496c81bfef9be5b

How are the properties of \cdot summarised in the definition of a field F ?

■ $(F - \{0\}, \cdot)$ is an abelian group.

Note 4

bc1d11a398434735a6129ece90078d0b

In the definition of a field F , what does 0 refer to?

■ The identity of F with respect to $+$.

Note 5

a12c4072b03f4f4385856eb63232dc6e

What is the key property that relates $+$ and \cdot in the definition of a field F ?

■ The distributive law.

Note 6

e20af7d49d0f467694122bf0aad50c59

The distributive law from the definition of a field F states that

$\{\{c1::$

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c), \quad \text{for all } a, b, c \in F.$$

$\}\}$

Note 7

34af1e3acbf4b2e8485bd9ddf265e4a

For any field F let $\{\{c2::F^\times\}\} = \{\{c1::F - \{0\}\}\}$.

Note 8

18535f79dcff4a67b32868a9f60b8f7e

Given $\{\{c3::\text{a prime } p,\}\}$ we shall denote $\{\{c1::\text{the field } \mathbb{Z}/p\mathbb{Z}\}\}$ as $\{\{c2::\mathbb{F}_p\}\}$ to emphasize that $\{\{c4::\text{it is a field.}\}\}$

Note 9

53ab9021abdc4aab9077b752f52df492

Given $\{\{c3::n \in \mathbb{Z}^+\}\}$ and $\{\{c4::\text{a field } F,\}\}$ $\{\{c1::\text{the general linear group of degree } n\}\}$ is denoted $\{\{c2::$

$$GL_n(F).$$

$\}\}$

Note 10

26483d8a0f29448db95af373c3315d8f

What are the elements of $GL_n(F)$?

■ All $n \times n$ matrices whose entries come from a field F and whose determinant is nonzero.

Note 11

62ca6e7bafed4c0fa4621e7fcb7a612d

What is the operation of $GL_n(F)$?

■ Matrix multiplication.

Note 12

ecd39cec434e4ca58d71efd99f59f652

Let F be a field. If $\{\{c2::|F| < \infty,\}\}$ then

$$\{\{c3::|F|\}\} = \{\{c1::p^m \text{ for some prime } p \text{ and an integer } m.\}\}$$

Note 13

4262c7c840fb4996904e2a18838f8766

Let F be a field. If $\{\{c4::|F| = q < \infty,\}\}$ then

$$\{\{c3::|GL_n(F)|\}\} = \prod_{k=\{\{c2::0\}\}}^{\{\{c2::n-1\}\}} \{\{c1::(q^n - q^k).\}\}$$

Note 14

81873bd4066c43069f33d507d19a4f29

Let F be a field. The subgroup of all the unit upper triangular matrices in $GL_3(F)$ is called the Heisenberg group over F .

Note 15

ab984848eb1941a4ba184e6bc8efece7

Let F be a field. The Heisenberg group over F is denoted $H(F)$.

Note 16

dfc23a9c6de94344a15a98b09a255950

Let F be a field. Then

$$|H(F)| = |F|^3.$$

Note 17

d23fde00126540ae999cadfb9f0101f4

Let $x \in H(\mathbb{R})$. If $x \neq 1$, then

$$|x| = \infty.$$

The Quaternion Group

Note 1

239ae951128a45148a7a0b069837604e

The quaternion group is denoted Q_8 .

Note 2

555bc9c4e6e549a8954f57e369620c61

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}.$$

Note 3

6e7c0944844b48afb9f531e5d1fa28c7

$$|Q_8| = 8.$$

Note 4

4227539ce42c4875a7adfb3ca6f82b3

In Q_8 , $1 \cdot x = x \cdot 1 = x$, for all x .

Note 5

fe801d8cadf94adc8af7a8f10209ed3b

In Q_8 , $(-1) \cdot x = x \cdot (-1) = -x$, for all x .

Note 6

3b0e08d205ac4eb59c5eb69b79b45201

In Q_8 , $(-1) \cdot (-1) = 1$.

Note 7

c779211682144018898526c5025c9048

In Q_8 , $i \cdot i = -1$.

Note 8

796029c2d52b43d6944db20f10fdd8af

In Q_8 , $j \cdot j = -1$.

Note 9

ec5bd7ed074a42d6ba94f6bd9da19392

In Q_8 , $k \cdot k = -1$.

Note 10

e38c1bab9ae74d96b1ad4505d46d0417

In Q_8 , $i \cdot j = k$.

Note 11

15482b24d8c34da580643a244f8080dc

$$\text{In } Q_8, \quad j \cdot k = \langle\langle c1::i \rangle\rangle.$$

Note 12

654c41a13a224d9f941e791b4ce340e1

$$\text{In } Q_8, \quad k \cdot i = \langle\langle c1::j \rangle\rangle.$$

Note 13

9be42c8a75764261a0ec49fd8d867350

$$\text{In } Q_8, \quad j \cdot i = \langle\langle c1:: -k \rangle\rangle.$$

Note 14

de5cd3f588fd4c59a098434677b65581

$$\text{In } Q_8, \quad k \cdot j = \langle\langle c1:: -i \rangle\rangle.$$

Note 15

b0e3385e5ab240d88ab165e2347bedc9

$$\text{In } Q_8, \quad i \cdot k = \langle\langle c1:: -j \rangle\rangle.$$

Note 16

34b82771d5ed4619b3024d89b76ed248

$$Q_8 = \langle\langle\langle c1::i, j \rangle\rangle\rangle$$

Note 17

e8cdf713f64b4e39b536f9b52b4ee716

$$\langle\langle c3::Q_8 \rangle\rangle = \langle i, j \mid \langle\langle c1::i^2 = j^2, \rangle\rangle \langle\langle c2::ij = ji^{-1} \rangle\rangle \rangle.$$